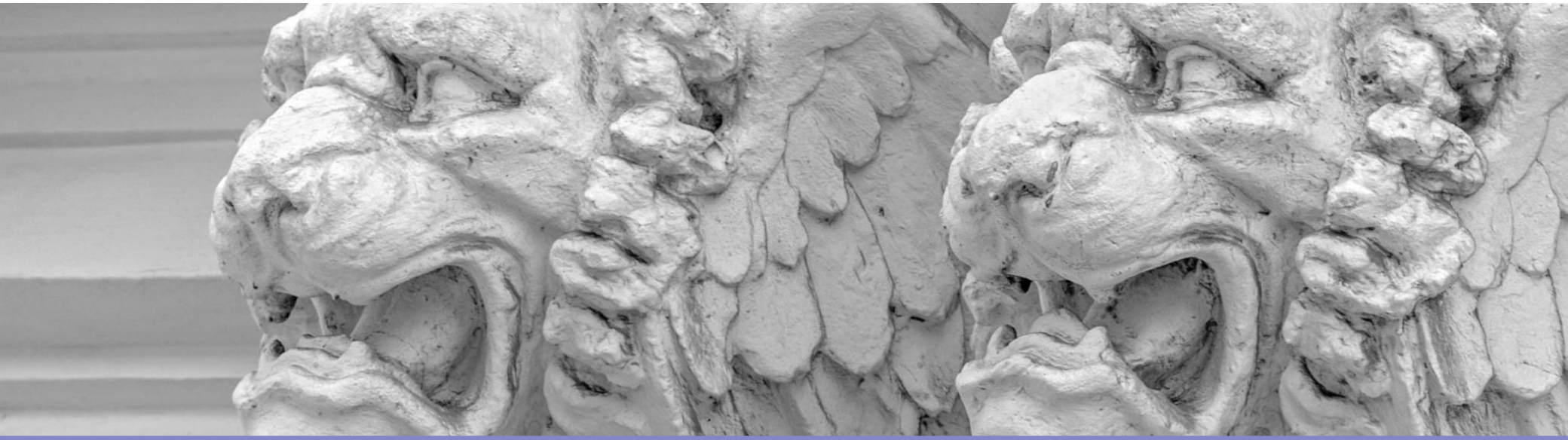
Банк России
Центральный банк Российской Федерации

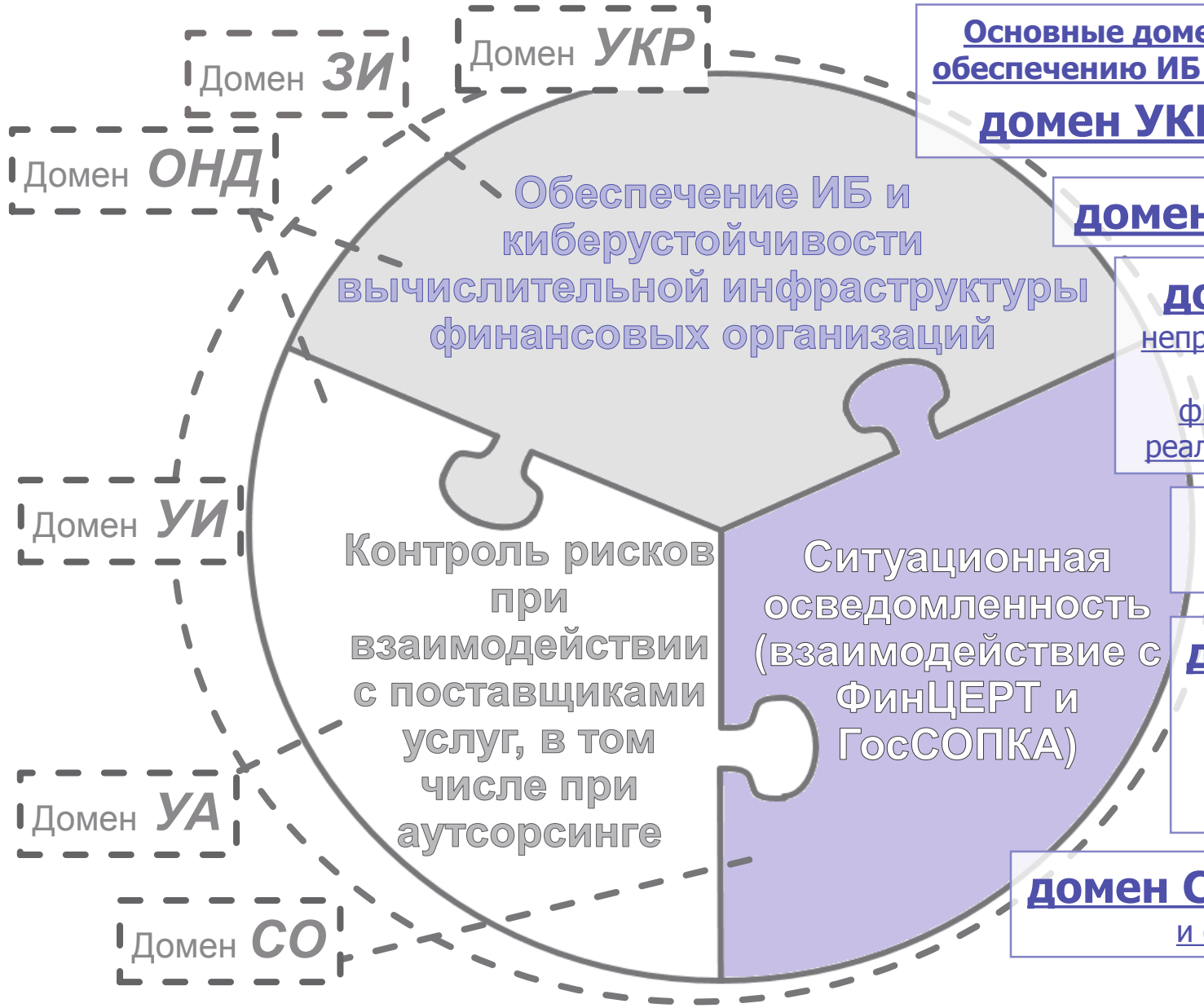


Стандартизация кибербезопасности

Выборнов Андрей Олегович

заместитель директора – начальник Управления
Департамента информационной безопасности Банка России

27.07.2018



Основные домены видов деятельности по обеспечению ИБ и управлению киберриском:

домен УКР – «управление киберриском»

домен ЗИ – «защита информации»

домен ОНД – «обеспечение непрерывности выполнения бизнес и технологических процессов финансовых организаций в случае реализации информационных угроз»

домен УИ – «управление инцидентами ИБ»

домен УА – «управлением киберриском при аутсорсинге и использовании сторонних информационных услуг (сервисов)»

домен СО – «мониторинг киберрисков и ситуационная осведомленность»

НОРМАТИВНАЯ МЕТОДОЛОГИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ

Методологическая деятельность

совершенствование комплекса отраслевых документов, устанавливающих требования к обеспечению ИБ и управлению киберриском, для обеспечения наличия отраслевой методологической основы деятельности Банка России и финансовых организаций по противодействию актуальным информационным угрозам и компьютерной преступности

Основные домены видов деятельности по обеспечению ИБ и управлению киберриском:

домен УКР – «управление киберриском»

домен ЗИ – «защита информации»

домен СО – «мониторинг киберрисков и ситуационная осведомленность»

домен ОНД – «обеспечение непрерывности выполнения бизнес и технологических процессов финансовых организаций в случае реализации информационных угроз»

домен УА – «управлением киберриском при аутсорсинге и использовании сторонних информационных услуг (сервисов)»

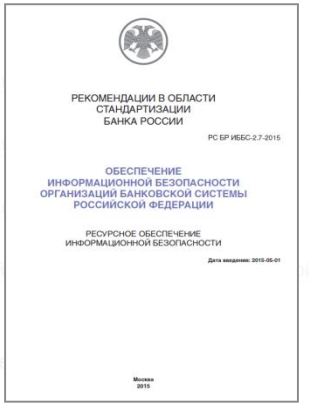
домен УИ – «управление инцидентами ИБ»

Разработано:

2 ГОСТ Р

5 СТО БР ИББС

8 РЕКОМЕНДАЦИЙ



Нормативная правовая деятельность

Область применения:

- защита информации при осуществлении переводов денежных средств;
- осуществление депозитарной деятельности;
- проведение организованных торгов;
- деятельность специализированных депозитариев;
- осуществление деятельности по ведению реестра владельцев ценных бумаг;
- создание и эксплуатация единой автоматизированной системы и перечнях видов информации, предоставляемой страховщиками;
- сохранность и защита информации, полученной в процессе деятельности кредитного рейтингового агентства;
- информационные технологии, используемые операторами услуг платежной инфраструктуры, для целей признания платежной системы национально значимой платежной системой
- обеспечение бесперебойности и непрерывности функционирования официальных сайтов страховщиков и профессионального объединения страховщиков в информационно-телекоммуникационной сети «Интернет» в целях заключения договоров обязательного страхования в виде электронных документов

НОРМАТИВНАЯ МЕТОДОЛОГИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ

Домен «управление киберриском» (домен УКР)

ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение информационной безопасности и управление риском реализации информационных угроз. Общие положения» (ввод в действие в 2019)

ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение информационной безопасности и управление риском реализации информационных угроз. Методика оценки соответствия» (ввод в действие в 2020)

Домен «защита информации» (домен ЗИ)

ГОСТ Р «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер защиты информации» (ввод в действие в 2018)

ГОСТ Р «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (ввод в действие в 2018)

Домен «управление инцидентами ИБ» (домен УИ)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управление инцидентами ИБ. Требования и меры организации» (ввод в действие в 2019)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управление инцидентами ИБ. Сбор и анализ технических данных» (ввод в действие ГОСТ в 2019)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управление инцидентами ИБ. Требования к организации взаимодействия с ФинЦЕРТ Банка России» (ввод в действие ГОСТ в 2019)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управление инцидентами ИБ. Методика оценки соответствия» (ввод в действие ГОСТ в 2020)

Домен «управление киберриском при аутсорсинге и использование сторонних информационных услуг (сервисов)» (домен УА)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управлением риском информационных угроз при аутсорсинге и использовании информационных сервисов. Аутсорсинг» (ввод в действие СТО в 2018, ввод в действие ГОСТ в 2020)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управлением риском информационных угроз при аутсорсинге и использовании информационных сервисов. Использование информационных сервисов» (ввод в действие СТО в 2019, ввод в действие ГОСТ в 2021)

ГОСТ Р «Безопасность финансовых (банковских) операций. Управлением риском информационных угроз при аутсорсинге и использовании информационных сервисов. Методика оценки соответствия» (ввод в действие в 2021)

Домен «мониторинг киберрисков и ситуационная осведомленность» (домен СО)

ГОСТ Р «Безопасность финансовых (банковских) операций. Мониторинг киберрисков и ситуационная осведомленность. Требования и меры реализации» (ввод в действие СТО в 2019, ввод в действие ГОСТ в 2020)

ГОСТ Р «Безопасность финансовых (банковских) операций. Мониторинг киберрисков и ситуационная осведомленность. Методика оценки соответствия» (ввод в действие ГОСТ в 2021)

Домен «обеспечение непрерывности выполнения бизнес и технологических процессов финансовых организаций в случае реализации информационных угроз» (домен ОНД)

ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение непрерывности выполнения бизнес и технологических процессов. Требования и меры реализации» (ввод в действие СТО в 2020, ввод в действие ГОСТ в 2022)

ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение непрерывности выполнения бизнес и технологических процессов. Методика оценки соответствия» (ввод в действие ГОСТ в 2021)

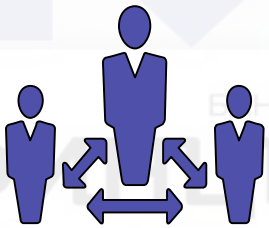
ВИДЫ ДЕЯТЕЛЬНОСТИ

Законотворческая деятельность

Разработан и введен в действие федеральный закон от 27 июня 2018 г. № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств», вступает в силу в октябре 2018 года.

Нормативная правовая деятельность

Указание Банка России от 7 мая 2018 г. N 4793-У «О внесении изменений в Положение Банка России от 9 июня 2012 года N 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», зарегистрировано в Министерстве юстиции Российской Федерации за № 51411 от 22.06.2018.



Методологическая деятельность

Разработан Стандарт Банка России о технологии подготовки, направлении и форматах электронных сообщений для информирования Банка России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Организационная деятельность

Реализация информационного обмена предполагается путем создания автоматизированной системы, используемой ФинЦЕРТ для повышения готовности противостоять информационным угрозам путем организации автоматизированного обмена информации:

об актуальных уязвимостях, информационных угрозах и компьютерных атаках;

о случаях совершения перевода (попытках совершения перевода) денежных средств без согласия клиента, включая обезличенную информацию о расчетных счетах физических лиц, используемых для «выведения» несанкционированно переведенных денежных средствах (счетах «дропов»).

Банк России
Центральный банк Российской Федерации

Благодарю за внимание!